Leibniz Rechenzentrum

der Bayerischen Akademie der Wissenschaften

Motivation: Warum ist Security wichtig?

Petra Eilfeld

2004-12-03

Inhalt:

Vielen Benutzer(inne)n und leider auch Systemverwalter(inne)n ist nicht bewusst, dass ***jede(r)*** *selbst ihren/seinen Beitrag zur Verbesserung der System- und Netzsicherheit leisten kann und aus* ***eigenem Interesse*** *auch unbedingt sollte.*
Außerdem werden Sicherheitsmaßnahmen bei "Kosten-/Nutzenrechnungen" oft unterschätzt, da die "Folgekosten" (Geld, Personal, juristische Probleme etc.) von eingetretenen Sicherheitsvorfällen entweder ganz übersehen oder unterbewertet werden.

Zum Glück sind Hacker nicht so genial und unbesiegbar, wie Sie vielleicht denken! Bereits mit relativ einfach umzusetzenden Maßnahmen und ein wenig Selbstdisziplin können Sie Ihre Sicherheit deutlich verbessern.

Was auch Ihnen passieren könnte

Erst einmal ein paar (hoffentlich) abschreckende Beispiele aus der Praxis (diese Vorfälle sind *wirklich* passiert !):

- Von einem sehr spektakulären Fall (http://www.heise.de/newsticker/data/jk-23.04.03-006/) wurde sogar in der Tagespresse berichtet: Ein "Witzbold" hatte im Namen eines Münchner Gärtners beim Online-Auktionshaus eBay (http://www.ebay.de/) Waren im Gesamtwert von rund 1,4 Millionen Euro ersteigert (u.a. ein Grundstück in Leipzig, ein Nobelauto, ein Ultraleichtflugzeug, ein Bild von Andy Warhol, einen externen Herzschrittmacher und einen ausgemusterten Geldtransporter).

  Wahrscheinlich wurde auf dem Rechner des legitimen eBay-Nutzers eingebrochen und dadurch dann ein Zugriff auf das eBay-Zugangspasswort möglich. Möglicherweise war der Gärtner aber auch zu sorglos im Umgang mit seinem Passwort.

  Bei einem ähnlichen zweiten Fall (http://www.heise.de/newsticker/data/jk-05.05.03-004/) gab es sogar Schäden in einer Gesamthöhe von 5,5 Millionen Euro.

- Eine bundesweit agierende Hackergruppe konnte einen Gesamtschaden von 750.000 Euro (http://www.heise.de/newsticker/data/dab-22.05.03-001/) verursachen, weil Unternehmen u.a. die vom Hersteller voreingestellten Schutz-PIN's ihrer Telefonvermittlungsanlagen nicht geändert hatten.

- Der Sohn eines Mitarbeiters fing sich beim Surfen am heimischen PC einen 0190-Dialer ein. Daraufhin erhielt der Mitarbeiter eine recht unangenehme Überraschung: Eine Telefonrechnung von mehreren hundert Euro.

- Ein Jurastudent gab seine Kennung an einen "hilfsbereiten" Kommilitonen weiter, damit dieser ihm ein geeignetes Profile einrichten konnte. Der Kommilitone benutzte die Gelegenheit, die Semesterarbeit des Studenten zu entwenden und als seine eigene abzugeben. Da der Dieb sämtliche Quellen gelöscht hatte, konnte der tatsächliche Autor seine Urheberschaft nicht beweisen und verlor durch eine deshalb erforderliche zweite Arbeit ein ganzes Semester.

- Ein Student verließ nach dem Diplom seinen Lehrstuhl. Seine Kennung blieb aber (mit dem ursprünglichen Passwort) bestehen. Kurz darauf wurde die Kennung geknackt, was zunächst nicht bemerkt wurde, da die Kennung ja inaktiv war. Der Täter benutzte die Kennung zur Verbreitung illegalen pornographischen Materials. Der ursprüngliche Inhaber der Kennung hatte größere Schwierigkeiten, seine Unschuld zu beweisen.

- Ein Patient litt unter komplexen Beschwerden. Die behandelnden Ärzte diskutierten via E-Mail über die Behandlung und verschickten dabei Patientendaten. Die Kennung eines der Ärzte wurde geknackt, die Daten gelangten in die Hände unerwünschter Dritter.

Warum ist System- und Netzsicherheit so wichtig ?

Seit Mitte 2001 hat weltweit die Aktivität der Hacker und der "Viren-/Würmerbastler" dramatisch zugenommen: Mitte 2002 ereigneten sich z.B. im Münchner Wissenschaftsnetz (MWN) oft an *einem Tag* so viele Sicherheitsvorfälle wie noch Anfang 2001 in *einem ganzen Monat !* Im Jahr 2004 waren es mehr als 600 Vorfälle.

Es ist eine **fatale Einstellung**, sich nicht mit System- und Netzsicherheit (Security [S.6]) zu befassen. Dies wird auch sofort klar, wenn man sich die möglichen **schwerwiegenden Folgen** vergegenwärtigt.
Direkte Folgen sind vielen Benutzer(inne)n noch einigermaßen bewußt (nicht zuletzt dadurch, dass Security auch schon zum Thema der Tagespresse geworden ist):

- Ist ein Rechner von einem Virus / Wurm verseucht bzw. durch einen Hacker kompromittiert, bleibt in den meisten Fällen nur eine komplette Neuinstallation des Betriebssystems und aller Anwendungsprogramme.
  Abgesehen vom Zeitverlust gehen dabei auch oft Daten verloren.

- Ein Hacker / Virus / Wurm kann absichtlich oder aus Versehen Daten verändern oder löschen.

  Dies ist natürlich besonders fatal, wenn es kurz vor Abgabe einer wichtigen Abschlussarbeit geschieht und man sich nicht um eine ausreichende Datensicherung (Backup) gekümmert hat.

- Wenn man sich einen 0190-Dialer unbemerkt einfängt, muss man sich auf eine Telefonrechnung von mehreren Hundert bis zu mehreren Zehntausend Euro gefasst machen!
  Auf diese Art wurden inzwischen schon einige Personen bzw. ganze Familien in den finanziellen Ruin getrieben.

- Ein geknackter Rechner kann als Ausgangspunkt für weitergehende Hackeraktivitäten dienen und damit anderen Rechnern und Personen schaden:

  - Ihr Rechner könnte als "Abhörstation" im lokalen Netz verwendet werden (z.B. um sich Kennungen und dazugehörige Passwörter zu beschaffen).

  - Oft benutzen Hacker einen geknackten Rechner als Sprungbrett, um weitere Rechner zu knacken.
    Wird der Einbruch *irgendwo* in der Kette entdeckt, macht man *Sie* für den Einbruch zumindest mitverantwortlich.
    Außerdem kann ein Hacker i.a. sehr viel leichter andere Rechner in *Ihrem lokalen Netz* knacken, wenn er *vorher* schon *Ihren Rechner übernommen hat* und ihn dann als *Sprungbrett* missbrauchen kann. Ein evtl. vorhandener Firewall zum Internet muss dann z.B. nicht mehr erst überwunden werden.
    Im Extremfall kann ein komplettes lokales Netz durch einen knackbaren Rechner von innen heraus "aufgerollt" werden.

- (Distributed) Denial of Service-Angriffe ((D)DoS-Attacks):
  Ein anderer Rechner wird mit unsinnigen oder fehlerhaften Aufträgen so intensiv beschäftigt, dass er seine eigentlichen Aufgaben nicht mehr erfüllen kann.

- Ihr Rechner könnte als "Verteilstation" missbraucht werden:
  - Copyright-geschütztes oder rechtlich bedenkliches Material (Pornografie, Bombenbauanleitungen etc.)
  - Viren, Würmer, Flames, Spams

Indirekte Folgen sind noch nicht so bekannt und treten vor allem dann ein, wenn der eigene geknackte Rechner zum Ausgangspunkt für weitergehende Hackeraktivitäten diente (siehe oben [S.2]):

- *Strafrechtliche* Folgen:

  Man kann in den Verdacht geraten, selbst der Verursacher zu sein. Dies kann bis zu einem polizeilichen Ermittlingsverfahren gegen Sie oder soger bis zu einer Gerichtsverhandlung führen. Selbst wenn sich Ihre Unschuld herausstellt, müssen Sie mit erheblichen Unannehmlichkeiten rechnen; z.B. kann es je nach Sachlage passieren, dass *Sie selbst* Ihre Unschuld beweisen müssen.

  Evtl. müssen Sie sich auch vorhalten lassen, dass Sie durch Ihre (grobe) Fahrlässigkeit eine Straftat erleichtert oder sogar erst ermöglicht haben.

- *Zivilrechtliche* Ansprüche und *finanzielle* Folgen:

  - Es wird zunehmend diskutiert, ob man sich durch Fahrlässigkeit mit schuldig macht. Geschädigte fangen inzwischen schon vereinzelt an, Rechnungen für die bei ihnen entstandenen Schäden zu verschicken!

  - Ein Hacker verschickt von Ihrem Rechner aus unter Ihrem Namen beleidigende E-Mails an Adressen aus Ihrem Adressbuch. Daraufhin werden Sie mit Beledigungsklagen konfontiert.

  - Ein Hacker startet *in Ihrem Namen* rechtsverbindliche Aktionen [S.1] , für deren Folgen dann *Sie geradestehen* müssen.

  - Durch Ihre Sorglosigkeit entstand Ihrer Firma ein großer Schaden (z.B. gelangten wichtige Betriebsgeheimnisse in den Besitz der Konkurrenz). Dies kann im schlimmsten Fall den Ruin Ihrer Firma oder Ihre fristlose Kündigung bedeuten (wenn Sie durch Ihren Fehler gegen Klauseln in Ihrem Arbeitsvertrag verstossen haben).

- *Organisatorische* und/oder *finanzielle* Folgen:

  - Der Provider kann den Vertrag kündigen.

  - Sie haben durch Ihre Fahrlässigkeit gegen die Benutzerordnung verstoßen und daraufhin wird Ihre Studentenkennung zeitweise oder sogar dauerhaft gesperrt.

- *Technische* Folgen:

  Ihr Rechner kann auf schwarze Listen geraten, wodurch dann bestimmte Dienste nicht mehr funktionieren. Dies wird z.B. bei E-Mail schon in großem Umfang zur Abwehr von Spam praktiziert.

- *Soziale* und/oder *finanzielle* Folgen:

  Man erleidet einen mehr oder weniger großen Imageverlust.

- *Soziale* Folgen:

  Man schadet seinem Umfeld.

- *Ärger und Arbeit:*

  Selbst wenn man glücklicherweise ohne größere Schäden davon kommt, wird man zumindest einige Arbeit in die Wiederherstellung eines "sauberen" Zustandes stecken müssen und sich dabei über die "überflüssige Fleißaufgabe" ärgern.

Fazit:

- *Heutzutage sollte man sich schon aus eigenem Interesse mit dem Gebiet der System- und Netzsicherheit (Security) vertraut machen.*

  Das Leibniz-Rechenzentrum (LRZ) möchte Ihnen dabei helfen und bietet deshalb eine ganze Reihe von Diensten im Bereich Security an.

- *Bei einem geknackten Rechner oder einer geknackten Benutzerkennung ist man meist nicht nur selbst betroffen, sondern gefährdet dadurch auch andere Benutzer, Rechner oder im schlimmsten Fall sogar ganze Netze (z.B. das lokale Netz der Firma, des Lehrstuhls oder des Instituts).*

Warum haben Hacker oft besonders leichtes Spiel ?

Hacker und Viren / Würmer haben i.a. nicht deshalb leichtes Spiel, weil es so viele "geniale" Hacker oder so exorbitant viele Sicherheitslücken in der Software gibt, sondern weil viel zu viele Benutzer(innen), Systemverwalter(innen) und schlimmstenfalls sogar gesamte Institutionen einfache Sicherheitsmaßnahmen nicht beachten oder unsachgemäß handhaben.
Möglicherweise erkennen Sie sich oder Bekannte in dem einen oder anderen der folgenden Zitate wieder:

- » Ich habe gar nicht angenommen, dass mein eben erst erstandener Rechner überhaupt unsicher sein könnte.
  Ich bin selbstverständlich davon ausgegangen, dass mir mein Fachhändler nur sichere Ware verkauft. «

- » Die Gefahren werden ja doch maßlos übertrieben; mir wird schon nichts passieren. «

- » Mein Rechner ist nur jeweils kurze Zeit über Modem mit dem Internet verbunden.
  Da kann doch sowieso nichts passieren. «

- » Woher sollte ich denn wissen, dass mein Web-Browser einen Bug hat und ich ihn deshalb hätte aktualisieren müssen? «

- » Kürzlich wurde ich durch einen Bericht in der Tageszeitung sehr beunruhigt.
  Ich habe aber nirgends eine *verständliche* Anleitung gefunden, wie ich meinen Rechner sicherer machen kann. «

- » Es ist mir einfach zu mühsam, die 50 Seiten Bedienungsanleitung für den Personal-Firewall durchzulesen.
  Da lasse ich es lieber gleich bleiben. «

- » Ich habe nichts zu verbergen, da mein Rechner eh' nichts Wichtiges oder Geheimes enthält; den Inhalt darf sowieso jeder lesen:
  - Es ist mir egal, ob mein Rechner geknackt ist oder nicht.
  - Mein Rechner ist deshalb für einen Hacker vollkommen uninteressant. «

- » Es ist mir zu unbequem, jedesmal für den Internet-Zugang ein Passwort einzugeben.
  Da lasse ich das Passwort lieber wie früher im Klartext auf die Platte schreiben. «

- » Ein kompliziertes Passwort kann ich mir nicht merken; und mehrere davon schon gar nicht. «

- » Mir hat niemand gesagt, dass man einen Viren-Scanner regelmäßig aktualisieren muss. «

- » Ich arbeite mit der Standardinstallation und habe keine Modifikationen vorgenommen. Wenn mein Rechner geknackt wird, schiebe ich einfach die Installations-CD ein und habe nach 20 Minuten wieder ein "sauberes" System. «

- » Ich würde ja gerne sehr viel mehr für die Sicherheit der Rechner in unserer Firma tun.
  Aber mein Chef meint, dass das neue Software-Paket viel wichtiger ist und dass der ganze "neumodische Security-Kram" sich eh' nicht rentiert. «

Warum ist die Anzahl der Angriffe so angestiegen ?

Es gibt im Wesentlichen drei Hauptübel, die Hackerangriffe unnötig erleichtern:

- Fehlerhafte Software in Kombination mit "Monokultur":

  Ähnlich wie bei biologischen Schädlingen in der Landwirtschaft breiten sich Computer-Viren / -Würmer etc. um so leichter und schneller aus, je einheitlichere Bedingungen sie vorfinden und je verbreiteter das Zielbetriebssystem ist. Im Moment betrifft dies vorwiegend die Windows-Welt, aber leider auch zunehmend Linux.

  Außerdem muss ein Hacker Zugriff auf das betreffende Zielbetriebssystem haben, wenn er für dieses Betriebssystem einen Virus / Wurm etc. entwickeln will. Deshalb wird es nur sehr wenige Viren für seltene Spezialbetriebssysteme geben.

- Hackerwerkzeuge im Internet:

  Selbst ein völlig unerfahrener Hacker hat heute schon erstaunliche Erfolgschancen. Es gibt nämlich zahlreiche Toolkits, die auch ohne größere Vorkenntnisse einfach zu bedienen sind und sehr wirkungsvoll sein können.

- Unwissenheit und/oder Sorglosigkeit von Benutzern, Administratoren und sogar Institutionen (siehe oben [S.4]):

  Viele Systeme enthalten so eklatante Sicherheitslücken, dass ein Einbruch unnötig einfach gemacht wird.

Begriffsbildung:
Was ist der Unterschied zwischen "Sicherheit" und "Security" ?

Selbst wenn man sich nur auf die EDV beschränkt, wird im Deutschen der Begriff **"Sicherheit"** in sehr verschiedenen Kontexten verwendet:

- Bei der **System- und Netzsicherheit** versucht man die Rechner und Netzkomponenten gegen direkte oder indirekte Eingriffe *unberechtigter* Personen zu schützen. Dabei werden bei indirekten Eingriffen i.a. Viren, Würmer, automatisierte Tools etc. eingesetzt.

  Dieser Aspekt wird im Englischen mit **"Security"** bezeichnet und beim "Security-Portal des LRZ" behandelt.

- Bei der **Datensicherung** sollen (irgendwie) verloren gegangene Daten durch geeignete Vorkehrungen wiederhergestellt werden können.

  Dies hat mit dem vorhergehenden Punk am Rande zu tun, da die betreffenden Daten z.B. von einem Hacker gelöscht oder manipuliert worden sein können.

- Bei der **Ausfallssicherheit** will man selbst bei ausgefallenen Komponenten einen (zumindest eingeschränkten) Betrieb gewährleisten.

- Beim **Datenschutz** kümmert man sich darum, dass Personen-bezogene Daten nur rechtlich einwandfrei verarbeitet werden.

- Bei der **Rechtssicherheit** sollen die "Spielregeln" möglichst klar und einheitlich sein und zumindest für längere Zeit gelten.

- Durch den **Rechtsschutz** will man z.B. erreichen, dass zugesicherte Eigenschaften (z.B. Performance) auch wirklich erfüllt sind, bzw. dass bei Nichterfüllung kein Schaden entsteht.

Da der deutsche Begriff *"Sicherheit"* so viele verschiedene Facetten besitzt, wird beim Security-Portal des LRZ oft der sehr viel präzisere englische Begriff *"Security"* verwendet.